

555, 340

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004 年 11 月 18 日 (18.11.2004)

PCT

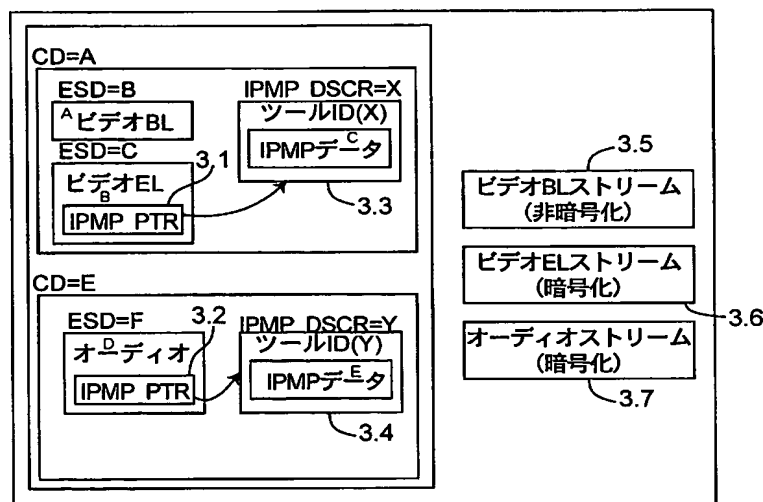
(10) 国際公開番号
WO 2004/100442 A1

- (51) 国際特許分類⁷: H04L 9/14, H04N 7/24 (74) 代理人: 河宮 治, 外(KAWAMIYA, Osamu et al.); 〒5400001 大阪府大阪市中央区城見 1 丁目 3 番 7 号 I M P ビル 青山特許事務所 Osaka (JP).
- (21) 国際出願番号: PCT/JP2004/006288
- (22) 国際出願日: 2004 年 4 月 30 日 (30.04.2004)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2003-131372 2003 年 5 月 9 日 (09.05.2003) JP
- (71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真 1 0 0 6 番地 Osaka (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF,
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): ジミン (JI, Ming). リュウジン (LIU, Jing). シェンシェン・メイ (SHEN, Sheng Mei). 妹尾 孝憲 (SENOH, Takanori).

[続葉有]

(54) Title: TRANSMITTER APPARATUS FOR MPEG-4 IPMP EXTENDED ISMA MEDIA STREAM

(54) 発明の名称: M P E G - 4 I P M P 拡張された I S M A 媒体ストリームの送信装置



A...VIDEO BL 3.5...VIDEO BL STREAM
B...VIDEO EL (UNENCRYPTED)
3.3...TOOL ID (X) 3.6...VIDEO EL STREAM
C...IPMP DATA (ENCRYPTED)
D...AUDIO 3.7...AUDIO STREAM
3.4...TOOL ID (Y) (ENCRYPTED)
E...IPMP DATA

(57) Abstract: An apparatus for transmitting an MPEG-4 IPMP extended ISMA media stream produces an ISMA media stream having an ISMA header and including, as a payload, contents, then embeds in the media stream an IPMP tool stream descriptor indicating, as a tool required for processing the contents, at least one tool selected from a group including an IPMP tool, an ISMACryp decryption tool, and a key management system (KMS) tool, and then transmits the ISMA media stream.

[続葉有]

WO 2004/100442 A1



BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

— 請求の範囲の補正の期限前の公開であり、補正書受領の際には再公開される。

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: MPEG-4 IPMP拡張されたISMA媒体ストリームを送信する装置であって、ISMAヘッダを有し、コンテンツをペイロードとして含むISMA媒体ストリームを構成し、前記コンテンツの処理に必要なツールとして、IPMPツールと、ISMACryp解読ツールと、鍵管理システム(KMS)ツールとを含む群から選ばれる少なくとも一つのツールを示すIPMPツールリスト記述子を前記媒体ストリームに埋め込み、前記ISMA媒体ストリームを送信する。

明 細 書

MPEG-4 IPMP拡張されたISMA媒体ストリームの送信装置

5 技術分野

本発明は、ISMA保護フレームワークについて互換可能なMPEG-4 IPMP拡張に関する。

背景技術

10 ここ数年、インターネットを介した映像や音声の配信が、メディアコンテンツ配信事業において益々期待されている。多くの標準化グループはこの問題に対する解決策を提供するため多大な努力をしてきた。インターネット・ストリーミング・メディア・アライアンス（ISMA：Internet Streaming Media Alliance）はそのようなグループの1つである。それは、IPフレームワークやインターネット中での利用に対して相互利用できる映像や音声システムを構築するためにベンダが利用できる、相互利用可能な既存のオープンスタンダードの利用に対するフレームワークを公表することによりその問題と取り組んでいる。その仕様は、既存のMPEG技術の利用を想定し、主として現段階の（但し、将来の適応や変更はMPEG-2やMPEG-7技術を含んでもよい）MPEG-4技術上へ焦点を当てている。

20 ISMAはまた暗号化フレームワーク、すなわち、ISMA媒体ストリームに対するISMACrypを定義する。このフレームワークは、新しいメディア、符号化に対して拡張可能であり、新しい暗号化変換に対してアップグレード可能であり、種々の鍵管理、セキュリティ、デジタル権利管理（DRM：Digital Rights Management）システムに対して利用可能である。それは、また、媒体ストリームのデフォルトの暗号化、及びISMA規格に対する媒体メッセージの認証を定義する。図1はISMAフレームワーク上のISMACrpt保護のアーキテクチャを示す図である。

ISMAが宣言しているように、2種類の受信装置が対象となる。すなわち、ISMA専用受信装置（ISMA-only receivers）とMPEGシステム対応受信装

置 (MPEG system-capable receivers) である。ここで、「ISMA専用受信装置」は、MPEG-4システムに対応可能な受信装置ではなく、つまり、MPEG-4の信号処理や、任意のMPEG-4 (エレメンタリ) 媒体ストリームに付随可能な制御 (エレメンタリ) ストリームを処理することができない受信装置である。これに対し、「MPEGシステム対応受信装置」は、ISMAに関連する情報とともにMPEG-4システムレイヤ情報を処理できる。MPEGシステム対応受信装置との相互利用性は、少なくとも最小レベルのMPEGシステム信号を含むMPEG IOD (Initial Object Description: 初期オブジェクト記述) により実現できる。IODはバイナリSDP (Session Description Protocol) 属性すなわちSDP IODとして含まれる。

ISMACrypはまた両方の種類の受信装置に利用できる。それはSDPメッセージ内のバイナリIODを拡張する。新しいシグナリング (通知) は、ISMAシグナリングにおいて検出される冗長度よりもむしろ非対称性を提供する: それは、SDP IODの「最小の」及び「基本の」通知パラメータを提供し、受信装置のMPEG-4 IPMPシステムとの相互利用性を最大にする。

しかしながら、IODに対して拡張して定義される現状のISMACrypは完全ではなく、最新のMPEG-4 IPMP拡張規格と一致していない。その結果、ISMAストリームはMPEG-4 IPMP拡張互換受信装置により正しく認識されない場合がある。例えば、ISMACryp規格は、IOD内のIPMP_Descriptorの存在がISMACryp保護を示すために使用されることを定義する。しかし、MPEG-4 IPMP拡張によれば、ツールリスト記述子 (Tool List Descriptor) は、IPMP保護がされていれば、IOD中に存在しなければならない。これらの不完全性及び不一致は、MPEG-4 IPMP拡張互換受信装置に対するISMAフレームワークの相互利用性を損なう恐れがある。

発明の開示

本発明は以下の問題を解決する。

ISMACryp規格は、SDP内のIODの拡張を通して、MPEG-4 I

PMPを用いた ISMACryp 保護の通知を定義する。IOD シグナリング (signaling) 内の IPMP_Descriptor の存在により、受信装置に対して、この媒体ストリームが保護されていることを知らせる。MPEG IPMP 非互換受信装置に関しては、それらは、その後、ストリームの所有者において適当な方法（例えば、単純にストリームを無視する）でストリームを処理できる。しかしながら、MPEG-4 IPMP 拡張規格は IPMP 保護を示すために IOD 内にツールリスト記述子が存在しなければならないことを規定する。その規格は IPMP 保護に対する IOD 内の IPMP 記述子の存在を保証しない。このため、ISMACryp で定義された通知方法 (signaling method) は、IOD がツールリスト記述子を持つが IPMP 記述子を持たない媒体ストリームの保護機構を正確に検出しないかもしれない。

さらに、MPEG-4 IPMP 拡張互換の受信装置で ISMA に関するデータ（例えば、IPMP データに付随する暗号化情報、KMS コンフィグレーション）の受信が可能となるようにするために、ISMACryp 規格は、IPMP 規格に基づいて定義された ISMACryp 記述子 (ISMACryp_Descriptor) によって IOD 内の IPMP 記述子を拡張した。しかしながら、MPEG-4 IPMP 規格の速い進展のため、IOD の文法は変更され、ISMACryp 規格がベースとした古いバージョンと異なるものとなった。これにより、IPMP コンテキスト内に格納される ISMA に関連するデータは、最新の MPEG-4 IPMP 拡張規格と互換性のある受信装置により認識され得ないおそれがあるという問題が生ずる。ISMA の既に定義済みのパラメータの変更を最小にしつつ、最新の MPEG-4 IPMP 拡張規格の整合性を保持するために、現行の MPEG-4 IPMP 拡張規格により ISMA に関連するデータを格納できる新しい機構が必要である。その機構は以前のバージョンの MPEG-4 IPMP 拡張規格と互換性を持つ。

シグナリングの問題を解決するため、本発明は、MPEG 初期オブジェクト記述子 (IOD) 内の ISMACryp 保護の存在を通知するシグナリング機構 (signaling mechanism) を定義する。ツールリストと IPMP 記述子が保護を知らせるために使用される。この手段は最新の MPEG-4 IPMP 拡張規格と互

換性があり、MPEGシステム対応ISMA受信装置に対し最大限の相互利用性を実現する。それはまた、コンテンツを再生するのに必要なツールを識別する柔軟な方法を与える。

本発明に係るMPEG-4 IPMP拡張されたISMA媒体ストリームを送信する装置では、ISMAヘッダを有し、コンテンツをペイロードとして含むISMA媒体ストリームを構成し、前記コンテンツの処理に必要なツールとして、IPMPツールと、ISMACryp解読ツールと、鍵管理システム(KMS)ツールとを含む群から選ばれる少なくとも一つのツールを示すツールリスト記述子を前記媒体ストリームに埋め込み、前記ISMA媒体ストリームを送信する。

ここで、IPMPツールとは、MPEG-4における知的財産保護管理(Intellectual Property Management and Protection: IPMP)ツールを意味し、たとえば、ストリーム中のコンテンツの認証、暗号復号、及び、電子透かし処理等のIPMP機能を実行するモジュールである。このIPMPツールは、ストリーム中に埋め込まれてもよいし、ストリームとは別に必要に応じて所定のサーバからネットワークを介してダウンロードすることによって取得してもよい。あるいはこれ以外の方法で外部から取得してもよい。

また、ISMACryp解読ツールは、ISMAにおける暗号化規格ISMACrypで暗号化されたコンテンツを解読するモジュールである。

さらに、鍵管理システム(Key Management System: KMS)ツールは、コンテンツを保護するための暗号鍵の発生/更新/廃止を行うツールであり、それぞれのコンテンツ保護方式毎に定められた方法に従う。この鍵管理システムツールは特に、ISMAにおいて規定される鍵管理システムに対応するツールを対象としており、例えば、暗号化の際に所定のデータ長ごとに鍵の入れ替えが行われた場合に、その復号化の際に暗号化の場合と同様に鍵の入れ替えを行うモジュールである。

なお、前記ツールリスト記述子を前記ISMA媒体ストリームのIODに埋め込んでもよい。

また、本発明に係るMPEG-4 IPMP拡張されたISMA媒体ストリームを送信する装置では、

I SMAヘッダを有し、コンテンツをペイロードとして含むI SMA媒体ストリームを構成し、

前記コンテンツの処理に必要なツールとして、I PMPツールと、I SMAC r y p 解読ツールと、鍵管理システム (KMS) ツールとを含む群から選ばれる
5 少なくとも一つのツールを示すI PMP記述子を前記媒体ストリームに埋め込み、
前記I SMA媒体ストリームを送信する。

さらに、前記I PMP記述子を指すI PMP記述子ポインタを前記I SMA媒体ストリームに埋め込むことが好ましい。ポインタを用いることで参照領域を別に確保できるので、I PMP記述子のサイズが拡張によって変化しても容易に対応できる。また、前記I PMP記述子ポインタを前記I SMA媒体ストリームの
10 E S記述子に埋め込んでもよい。

またさらに、前記I PMP記述子に加えて、前記少なくとも一つのツールを示すI PMPツールリスト記述子を前記I SMA媒体ストリームに埋め込むことが好ましい。

また、前記I SMAC r y p 解読ツールに用いるI SMAC r y p パラメータを、I PMP__D a t a __B a s e C l a s s から拡張したI SMAC r y p __D a t a 中に格納してもよい。さらに、前記I SMAC r y p __D a t a を、前記I PMP媒体ストリームのOD中に格納されるI PMP記述子中に格納してもよい。またさらに、前記I SMAC r y p __D a t a を、前記I PMP媒体スト
15 20 リーム中に格納されるI PMP__M e s s a g e 中に格納してもよい。

ところで、I SMAフレームワーク内ではI ODとODが構築される。I PMPツールリスト記述子がI OD内に埋め込まれ、I SMAC r y p 保護が存在するならば、I PMP記述子ポインタとI PMP記述子がI OD及びOD内に埋め込まれる。

I OD及びODが、MPEG-4システムを理解するI SMA受信装置にSDP I ODシグナリングによって送られる。受信装置では、I ODとODを解析する。I PMPツールが検出されたときに、受信装置はI SMAC r y p 保護が存在することを認識する。I PMP記述子ポインタとI PMP記述子が検出されたときに、受信装置は、どのストリームがどのツールによって保護されるのかを
25

知ることができる。

I S M Aフレームワーク内で、ストリームがI S M A C r y pにより保護されている場合、I S M A C r y pパラメータ（例えば、暗号識別子）はI S M A C r y p _ D a t a内に格納可能であり、I P M P記述子またはI P M Pストリー
5 ム内に配置可能である。パラメータの格納はM P E G - 4 I P M P拡張規格である。

受信装置側にて、I S M A C r y pに関するパラメータは、M P E G - 4 I P M P拡張互換方法で、I P M P記述子またはI P M Pストリームから抽出できる。それらのパラメータはI S M A C r y p記述ツールを構成するために使用できる。

10 本発明の採用により、I S M A保護フレームワークが、M P E G - 4 I P M P拡張互換受信装置との相互利用性を実現できる。

本発明はI O D内のツールリスト及びO D内のI P M P記述を利用してI S M A C r y p保護を通知するものである。そうすることにより、シグナリング方法が、柔軟にすることができ、また、最新のM P E G - 4 I P M P拡張規格に真に
15 互換性を持たせることができる。これにより、M P E Gシステム対応I S M A受信装置の相互利用を可能にする。

本発明はまたI P M P _ D a t a _ B a s e C l a s sから拡張されたI S M A C r y p _ D a t aを生成する。発明されたI S M A C r y p _ D a t aはI S M A C r y pパラメータを格納するために使用でき、実質的にI P M P記述子
20 またはI P M Pストリームのいずれかにおいて格納され得る。I S M A C r y pパラメータを格納することはM P E G - 4 I P M P拡張に準拠することになる。

図面の簡単な説明

図1は、I S M A C r y pアーキテクチャを示す図である。

25 図2は、M P E G - 4 I P M P拡張・コンテンツの構造を示す図である。

図3は、I P M P記述子を用いてI P M Pによる保護がされているコンテンツを含むストリームの構造を示すブロック図である。

図4の(a)は、図3で示すI S M Aストリームの構造を示す概略図であり、(b)は、(a)のE S記述子内の構造を示す拡大概略図である。

図5は、IPMP記述子ポインタを含まないISMAストリームの構造を示す概略図である。

図6は、エンコーダ側でISMA媒体ストリームを処理して発信するISMA媒体ストリームの第1の処理方法を示すフローチャートである。

5 図7は、エンコーダ側でISMA媒体ストリームを処理して発信するISMA媒体ストリームの第2の処理方法を示すフローチャートである。

図8は、エンコーダ側でISMA媒体ストリームを処理して発信するISMA媒体ストリームの第3の処理方法を示すフローチャートである。

10 図9は、デコーダ側で受信したストリームの処理方法を示すフローチャートである。

発明を実施するための最良の形態

1. IPMP拡張・シグナリング

15 現行のISMACrypは、ISMA専用MPEG受信装置及びMPEG受信装置に対するSDP IODシグナリングをサポートする。ISMA専用受信装置は、SDP FMTPシグナリング・パラメータのみを受け取るが、SDP IODは、ストリームがISMACryp保護（最小のIPMPシグナリング）を有することを、任意のMPEG受信装置に通知しなければならない。KMSが、SDP IOD（基本IPMPシグナリング）内のIPMPシグナリングのみを用いてISMACrypシグナリングを知らせても良い。

20 本明細書はMPEG-4 IPMP拡張と互換性のある文法を提供する。最小の努力で、ISMACrypが、MPEG-4 IPMP拡張との互換性を容易に実現することができ、より柔軟な保護手段を提供する。

最小IPMP-Xシグナリング

25 IPMP拡張はIOD内のIPMPツールリスト記述子を定義する。IPMPツールリスト記述子は後の処理において必要なIPMPツールのリストを特定する。MPEG-4 IPMP拡張によれば、IPMP保護があるときは、ツールリスト記述子はIOD内に存在しなければならない。そして、最初のIPMP-Xシグナリングに関し、この目的を達成するために、IPMP記述子の代わりにI

OD内のI PMPツールリスト記述子を使用することを提案する。

暗号化及びKMS情報転送を規定する現行のI S M A C r y p仕様によれば、少なくとも2つのツールがM P E G I P M Pツールリスト記述子内に存在する必要がある。第1はKMSツールであり、第2はI S M A記述ツールである。M P E G I P M Pツールリスト内のI S M A C r y pツールの存在は、I S M A C r y p保護を知らせる。

I S M A C r y pツールによるツールリスト記述子 (Tool List Descriptor) の例を以下の表1に示す。

表1

		IPMP ToolListDescriptor	
1	8	IPMP ToolListDescTag	0x60
2	16	Descriptor size	
		IPMP Tool	
3	8	IPMP ToolTag	0x61
4	16	Descriptor size	
5	128	IPMP_ToolID	各サービスプロバイダによりそれぞれのKMSツールに割当てられた値
6	1	isAltGroup	0
7	1	isParametric	0
8	6	reserved	0b0000.00
9	8	Tool URL size	
10		Tool URL	
		IPMP Tool	
11	8	IPMP ToolTag	0x61
12	16	Descriptor size	
13	128	IPMP_ToolID	ISMA解読ツールに割当てられた値
14	1	isAltGroup	0
15	1	isParametric	0
16	6	reserved	0b0000.00
17	8	Tool URL size	
18		Tool URL	

I PMPツールリストが図2に示すMPEG-4 I PMP拡張のコンテンツ構

造に示されている。IPMPツールリスト(2.1)を使用することは、ISMA C r y p保護の存在の通知を容易にするだけではなく、ツールを特定する際に大きな柔軟性を与える。ツールリスト内のIPMPツールは3つの方法で特定できる。第1の方法は、固定の128ビットのIPMPツールID(2.2)(登録認証機関によって割り当てられた値)を使用することである。第2の方法は、互いに等価な代替ツール(2.3)を示すIPMPツールIDのリストを使用することである。そうすることにより、端末は、それ自身のツールを選択する際により大きな柔軟性を持つことができる。最後の方法は、IPMPツールが満たさねばならない規準を記述するパラメトリック記述(2.4)を使用することである。この場合、端末は必要な機能を実現するためのツールを選択する際により大きな自由度を持つことができる。

基本IPMP-Xシグナリング

MPEGシステム対応受信装置に関し、IPMPに関連する処理を行なうためにより多くのIPMP情報が必要である。より対応性のあるMPEGIPMP拡張・シグナリングについては、以下のIPMPシグナリングが基礎として採用されなければならない。セクション2において説明したツールリストとともに、それらはMPEG互換受信装置が必要なベース情報を提供する。暗号化されたエレメンタリストリームに対し、ES記述子に対応するそれらは以下の表2に示すようにIPMP記述子ポインタを含まなければならない。

表2

記述子名			
フィールド ド番号	サイズ (ビット)	フィールド名	値
		IPMP_DescriptorPointer	
1	8	IPMP_DescriptorPointer tag	10
2	8	descriptor size	5
3	8	IPMP_DescriptorID	0xFF
4	16	IPMPX_DescriptorID	0x0002 / 0x0003
5	16	IPMP_ES_ID	0x0000

このIPMP拡張保護シグナリングの概念が図3に示されている。ES記述子内のこの記述子ポインタ（3. 1、3. 2）の存在は、この記述子に関連するストリームが保護されており、参照されたIPMP記述子（3. 3、3. 4）にて規定されるIPMPツールにより管理されていることを示している。この参照されたIPMP記述子は、以下の表3に示すオブジェクト記述子中に格納されなければならない。

表3

記述子名			
フィールド番号	サイズ (ビット)	フィールド名	値
		IPMP Descriptor	
1	8	IPMP_Descriptor_tag	11
2	8	descriptor_size	23
3	8	IPMP_DescriptorID	0xFF
4	16	IPMPS_Type	0xFFFF
5	16	IPMP_DescriptorIDEx	0x0002 / 0x0003
6	128	IPMP_ToolID	ISMA解読ツールに割当てられた値
7	8	ControlPointCode	0x01 (デコードバッファとデコーダ間)
8	8	SequenceCode	0x80

また、IODは以下のIPMP記述子ポインタを含まなければならない。以下の表4の例では、参照された記述子内に示された特別なDRMツール（例えば、

5 鍵管理システムツール（Key Management System Tool））が全体的な範囲で事例を挙げて裏付けられなければならないことが記述されている。鍵管理システムツールは、コンテンツを保護するための暗号鍵の発生／更新／廃止を行うツールでそれぞれの保護方式毎に定められた方法に従う。

表4

記述子名			
フィールド 番号	サイズ (ビット)	フィールド名	値
		IPMP_DescriptorPointer	
1	8	IPMP_DescriptorPointer tag	10
2	8	descriptor size	5
3	8	IPMP_DescriptorID	0xFF
4	16	IPMP_DescriptorIDex	0x0001
5	16	IPMP_ES_ID	0x0000

上記のIPMP記述子ポインタは、IPMP_DescriptorIDex
が0x0001であるIPMP記述子を示す。そして、規定されたIPMP記述
5 子はIOD中に存在する必要がある。KMSに関し、記述子の制御ポイントは全
体的な範囲を示す0x00に設定されなければならない。

表 5

記述子名			
フィールド 番号	サイズ (ビット)	フィールド名	値
		IPMP_DescriptorPointer	
1	8	IPMP_DescriptorPointer tag	10
2	8	descriptor size	5
3	8	IPMP_DescriptorID	0xFF
4	16	IPMP_DescriptorIDex	0x0001
5	16	IPMP_ES_ID	0x0000

2. IPMP拡張互換法における ISMACryp の格納

ISMACryp はストリームの暗号化を記述するために 1 組のパラメータを使用する。IPMP 拡張互換法により格納されたパラメータを搬送するために、ISMACryp_Data が、IPMP_Data_BaseClass に
 5 いて定義された IPMP-X から拡張される。IPMP_Data_BaseClass は MPEG-4 IPMPX で以下のように定義される。

```
abstract aligned(8) expandable(228-1) class IPMP_Data_BaseClass:
```

```
    bit(8) tag=0 .. 255
```

```
{
```

```
10     bit(8)    Version;
```

```
    bit(32)    dataID;
```

```
    // Fields and data extending this message.
```

```
}
```

ISMACryp_Data は上記のベースクラスからユーザが定義してい
 15 ないタグを用いて拡張できる。データは、パラメータを搬送するそれ自身の組のフィールドを持つことができる。これにより、同じコンテンツストリームを解釈する異なる ISMA 端末間の相互利用が保証される。

この ISMACryp_Data は、標準的な方法では 2 つの場所に格納され
 20 得る。第 1 は IPMP 記述子の中に格納することである。ISMACryp_Data を有する IPMP 記述子の例を以下の表 6 に示す。

表 6

記述子名			
フィールド 番号	サイズ (ビット)	フィールド名	値
		IPMP_Descriptor	
1	8	IPMP_Descriptor tag	11
2	8	descriptor size	23
3	8	IPMP_DescriptorID	0xFF
4	16	IPMPS_Type	0xFFFF
5	16	IPMP_DescriptorIDEx	0x0002 / 0x0003
6	128	IPMP_ToolID	ISMA解読ツールに割当てら れた値
7	8	ControlPointCode	0x01 (デコードバッファと デコーダ間)
8	8	SequenceCode	0x80
		ISMACryp_Data	
7	8	ISMACryp_DataTag	定義必須
8	8	data size	20
9	8	Cipher-suite	暗号識別子
11	4	IV-length	初期ベクトルのバイト長
12	2	Delta-IV-length	AUに基いた初期ベクトルの バイト長
13	1	Selective-encryption	1 (選択的な暗号化が使用さ れた場合)
14	1	Key-indicator-per-Au	1 (複数の鍵指示情報が 1 パ ケット内に表れた場合)
15	8	Key-indicator-length	鍵指示情報のバイト長

ISMACryp_Dataを格納する第2の方法は、それをペイロードとしてIPMPメッセージ(IPMP_Message)に格納することである。IPMPメッセージは、MPEG-4 IPMP拡張において定義されるIPMPストリーム内に実質的に格納される。

```

5  aligned(8) expandable(228-1) class IPMP_Message
    {
        bit(16)    IPMPS_Type;
        if (IPMPS_Type == 0)
10     (
            bit(8) URLString[sizeofInstance-2];
        )
        else (if (IPMPS_Type == 0x0001)
15     (
            bit(16) IPMP_DescriptorID;
                IPMP_Data_BaseClass IPMP_ExtendedData[]
            } else {
                bit(8) IPMP_data[sizeofInstance-2];
            }
20     }

```

以下の表7の例は、IPMPメッセージがISMACryp_Dataを格納している場合のIPMPメッセージの文法を示す。IPMP_DescriptorIDexを有するIPMP記述子内で規定されるIPMPツールは、IPMPメッセージの目的である。

表7

フィールド 番号	サイズ (ビット)	フィールド名	値
		IPMP Message	
1	16	message size	
2	16	IPMPS_Type	0x0001
3	16	IPMP_DescriptorIDEx	
		ISMACryp Data	
4	8	ISMACryp_DataTag	定義必須
5	8	data size	20
6	8	Cipher-suite	暗号識別子
7	4	IV-length	初期ベクトルのバイト長
8	2	Delta-IV-length	AUに基いた初期ベクトルのバイト長
9	1	Selective-encryption	1 (選択的な暗号化が使用された場合)
10	1	Key-indicator-per-Au	1 (複数の鍵指示情報が1パケット内に表れた場合)
11	8	Key-indicator-length	鍵指示情報のバイト長

図4の(a)は、図3に示すISMA媒体ストリームの構造を示す概略図であり、図4の(b)は、(a)のIOD及びES記述子の詳細な構造を示す拡大概略図である。ISMA媒体ストリームでは、ISMAヘッダを有し、コンテンツをペイロード3.5、3.6、3.7として含んでいる。また、図4の(b)に示すように、IODのES記述子にはIPMP記述子3.3、3.4が示されており、IPMP記述子ポインタ3.1、3.2によってそれぞれのIPMP記述

子 3. 3、3. 4は参照されている。各 I PMP 記述子 3. 3、3. 4には、I PMP ツールリスト記述子が含まれており、この I PMP ツールリスト記述子には各コンテンツの処理に必要なツールとして、I PMP ツールと、I S M A C r y p 解読ツールと、鍵管理システムツールとを含む群から選ばれる少なくとも一つのツールを特定するツール I D が示されている。

図 5 は、I PMP 記述子は含むが、I PMP 記述子ポインタを含まない I S M A ストリームの構造を示す概略図である。この I S M A 媒体ストリームでは、I PMP 記述子の中の I PMP ツールリスト記述子に各コンテンツの処理に用いられるツールを特定するツール I D が示されている。

図 6 は、送信機（エンコーダ）側での I S M A 媒体ストリームの第 1 の処理方法を示すフローチャートである。以下に、送信機側での I S M A 媒体ストリームの第 1 の処理方法について説明する。

（a）I S M A ヘッダを有し、コンテンツをペイロードとして持つ I S M A 媒体ストリームを構成する（S 0 1）。

（b）各コンテンツの処理に必要なツールとして、I PMP ツールと、I S M A C r y p 解読ツールと、鍵管理システムツールとを含む群から選ばれる少なくとも一つのツールを示す I PMP ツールリスト記述子を I S M A 媒体ストリームの I O D に埋め込む（S 0 2）。具体的には、I PMP ツールリスト記述子にツール I D を記載する。

（c）I S M A 媒体ストリームを送信する（S 0 3）。

図 7 は、送信機（エンコーダ）側での I S M A ストリームの第 2 の処理方法を示すフローチャートである。以下に、送信機側での I S M A ストリームの第 2 の処理方法について説明する。

（a）I S M A ヘッダを有し、コンテンツをペイロードとして持つ I S M A 媒体ストリームを構成する（S 0 4）。

（b）各コンテンツの処理に必要なツールとして、I PMP ツールと、I S M A C r y p 解読ツールと、鍵管理システムツールとを含む群から選ばれる少なくとも一つのツールを示す I PMP 記述子を I S M A 媒体ストリームに埋め込む（S 0 5）。具体的には、I PMP 記述子にツール I D を記載する。

(c) IPMP記述子を指すIPMP記述子ポインタをISMA媒体ストリームのES記述子に埋め込む(S06)。

(d) ISMAストリームを送信する(S07)。

さらに好ましいのは、図8に示すように、上記IPMP記述子を埋め込むこと
5 (S10)に加えて、上記ツールを示すIPMPツールリスト記述子をさらにISMA媒体ストリームのIODに埋め込むこと(S09)である。ISMA媒体ストリームにコンテンツの処理に必要なツールを示すIPMP記述子とIPMPツールリスト記述子とをそれぞれ埋め込むことで、様々なISMA受信機において対応可能となる。

10 図9は、ISMA受信機側(デコーダ)で受信したストリームの処理方法を示すフローチャートである。以下に、ISMA受信機側でのストリームの処理方法について説明する。

(a) ストリームを受信する(S21)。

15 (b) 受信したストリームがISMA媒体ストリームか否かをチェックする(S22)。具体的には、ストリームにISMAヘッダが存在するか否かによってISMA媒体ストリームか否かを判断する。ISMA媒体ストリームではない場合にはそのまま終了する。

(c) 次に、IPMP記述子ポインタがあるか否かをチェックする(S23)。

20 (d) IPMP記述子ポインタがある場合には、そのポインタの指すアドレスのIPMP記述子を読み出す(S24)。

(e) IPMP記述子の内容に従ってストリームに含まれるペイロード(コンテンツ)を解読する(S25)。例えば、図4の(b)に示すように、IPMPポインタ3.1で指すIPMP記述子3.3の中に記載されたツールリストのツールIDに対応するツールを立ち上げて、ペイロードC3.6を暗号解読する。

25 (f) IPMP記述子ポインタがない場合には、そのまま読み出してIPMP記述子があるか否かをチェックする(S26)。IPMP記述子ポインタに対応していないISMA受信機用に構成されたISMA媒体ストリームではIPMP記述子ポインタを設けずにIPMP記述子が配置されている。そこで、このような場合にも直接にIPMP記述子を読み出すことができる。例えば、図5に示す

I SMA媒体ストリームの場合には、I PMP記述子ポインタはなく、I PMP記述子の中で、I PMPツールリスト記述子にツールIDが記載されている。この場合にも、ツールIDを読み出すことでペイロードC（コンテンツ）が保護されていることがわかる。

- 5 (g) I PMP記述子がある場合には、それを読み出す（S 2 7）。その後、ステップS 2 5に移行する。I PMP記述子がない場合には、終了する。

なお、本発明は、様々な実施の形態に示されている以下の構成をとることができる。第1の構成によれば、I SMAコンテンツプロバイダ側で、MPEG-4 I PMP拡張を用いたI SMA媒体ストリームを柔軟に保護する装置であって、

- 10 前記コンテンツの処理に必要なI PMPツールのリストを示すためにツールリスト記述子をIODに埋め込み、

ツールリスト中に規定されたツールの中から1つが、I SMA暗号化—解読ツールに割り当てられたツールIDを有し、

- 15 ツールリスト中に規定されたツールの中から1つが、鍵管理システム（KMS）ツールに割り当てられたツールIDを有し、

前記2つのツールのいずれかの存在がI SMA暗号化保護の存在を知らせることを特徴とする。

第2の構成によれば、IOD中のツールリストを用いてI SMA暗号化保護を知らせ、さらに、

- 20 媒体ストリームが保護されていることを示すためにI PMP記述子ポインタを媒体ストリームのES記述子に埋め込み、

前記I PMP記述子ポインタによって参照されるI PMP記述子がI SMA暗号化—解読ツールのツールIDを有することを特徴とする。

- 25 第3の構成によれば、I SMAコンテンツプロバイダ側で、MPEG-4 I PMP拡張を用いたI SMA媒体ストリームを柔軟に保護する装置であって、

I PMP__Data__BaseClassから拡張したI SMACryp__Data中に、I SMACrypパラメータを格納し、

I SMACryp__Dataを、OD中に実質的に格納されるI PMP記述子中に格納する、ことを特徴とする。

第4の構成によれば、ISMAコンテンツプロバイダ側で、MPEG-4 IPMP拡張を用いたISMA媒体ストリームを柔軟に保護する装置であって、

IPMP_Data_BaseClassから拡張したISMACryp_Data中にISMACrypパラメータを格納し、

5 ISMACryp_Dataを、IPMPストリーム中に実質的に格納されるIPMP_Message中に格納する、ことを特徴とする。

上述の通り、本発明は好ましい実施形態により詳細に説明されているが、本発明はこれらに限定されるものではなく、以下の特許請求の範囲に記載された本発明の技術的範囲内において多くの好ましい変形例及び修正例が可能であることは
10 当業者にとって自明なことであろう。

請 求 の 範 囲

1. MPEG-4 IPMP拡張されたISMA媒体ストリームを送信する装置であって、

5 ISMAヘッダを有し、コンテンツをペイロードとして含むISMA媒体ストリームを構成し、

前記コンテンツの処理に必要なツールとして、IPMPツールと、ISMACryp解読ツールと、鍵管理システム(KMS)ツールとを含む群から選ばれる少なくとも一つのツールを示すIPMPツールリスト記述子を前記媒体ストリー

10 ムに埋め込み、

前記ISMA媒体ストリームを送信する装置。

2. 前記IPMPツールリスト記述子を前記ISMA媒体ストリームのIODに埋め込むことを特徴とする請求項1に記載の送信装置。

3. MPEG-4 IPMP拡張されたISMA媒体ストリームを送信する装置であって、

15

ISMAヘッダを有し、コンテンツをペイロードとして含むISMA媒体ストリームを構成し、

前記コンテンツの処理に必要なツールとして、IPMPツールと、ISMACryp解読ツールと、鍵管理システム(KMS)ツールとを含む群から選ばれる少なくとも一つのツールを示すIPMP記述子を前記媒体ストリームに埋め込み、

20

前記ISMA媒体ストリームを送信する装置。

4. 前記IPMP記述子を指すIPMP記述子ポインタを前記ISMA媒体ストリームに埋め込むことを特徴とする請求項3に記載の送信装置。

5. 前記IPMP記述子ポインタを前記ISMA媒体ストリームのES記述子に埋め込むことを特徴とする請求項3に記載の送信装置。

25

6. 前記少なくとも一つのツールを示すIPMPツールリスト記述子を前記IPMP記述子とは別に前記ISMA媒体ストリームに埋め込むことを特徴とする請求項3から5のいずれか一項に記載の送信装置。

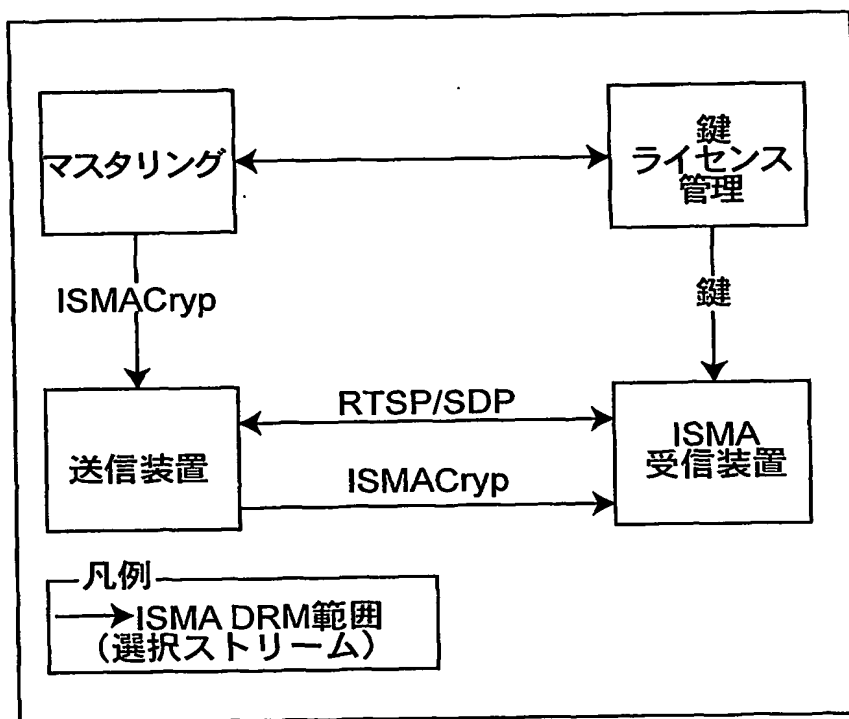
7. 前記ISMACryp解読ツールに用いるISMACrypパラメータを、

IPMP__Data__BaseClassから拡張したISMACryp__Data中に格納することを特徴とする請求項1から6のいずれか一項に記載の送信装置。

5 8. 前記ISMACryp__Dataを、前記IPMP媒体ストリームのOD中に格納されるIPMP記述子中に格納することを特徴とする請求項7に記載の送信装置。

9. 前記ISMACryp__Dataを、前記IPMP媒体ストリーム中に格納されるIPMP__Message中に格納することを特徴とする請求項7に記載の送信装置。

図1



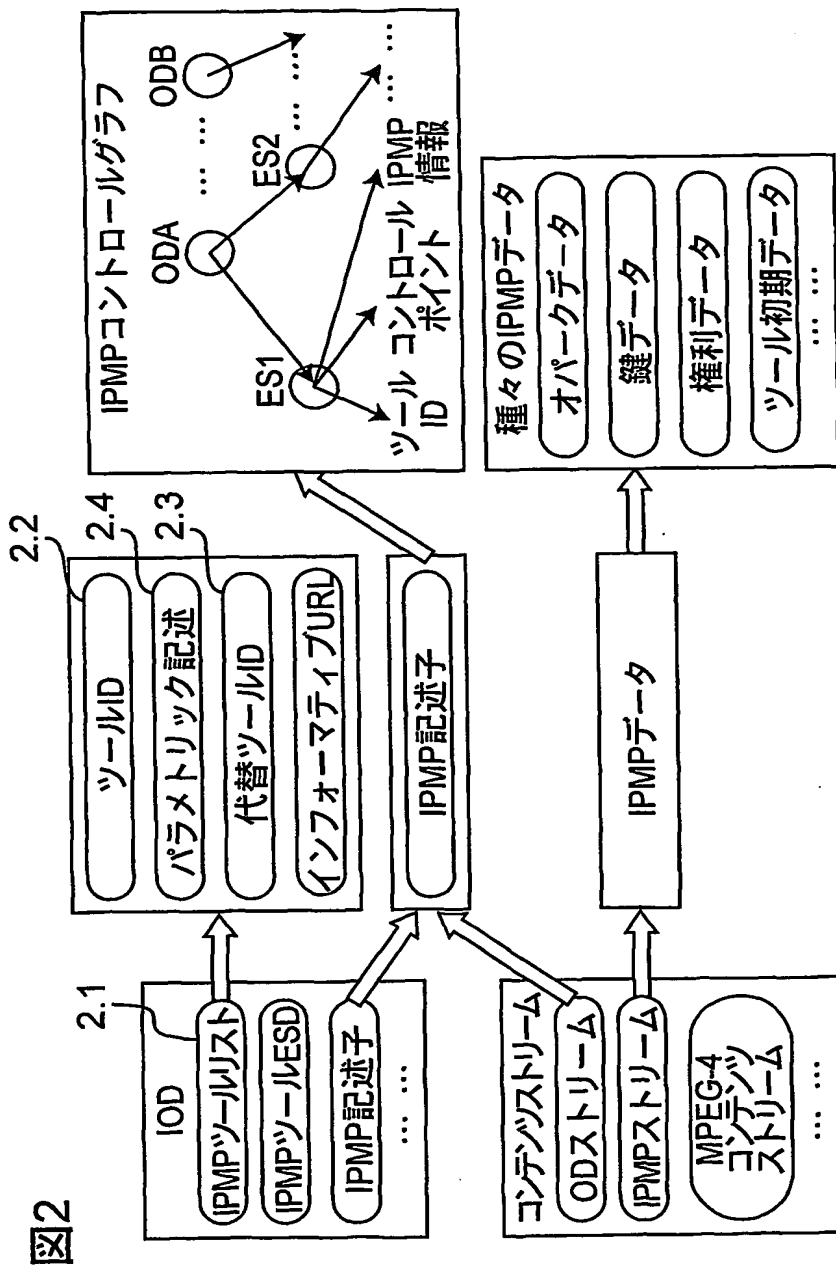
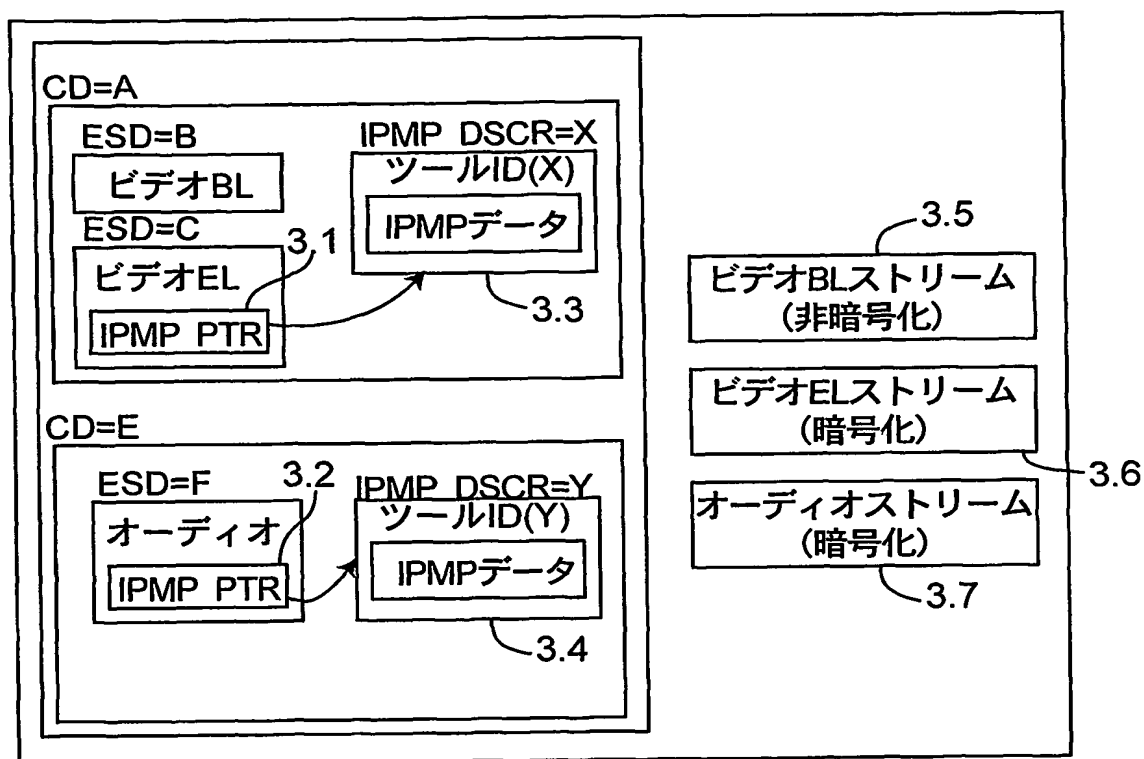


図3



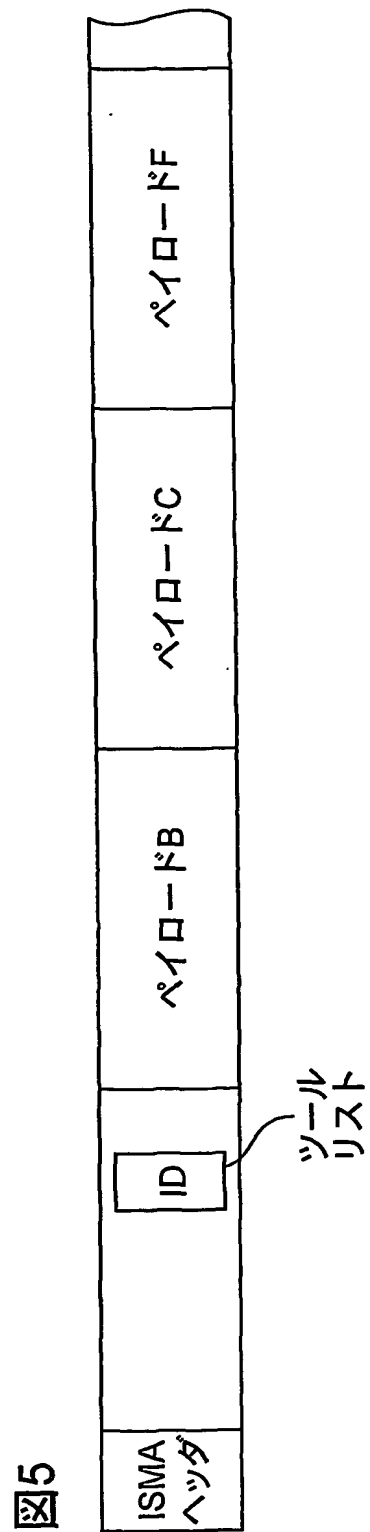
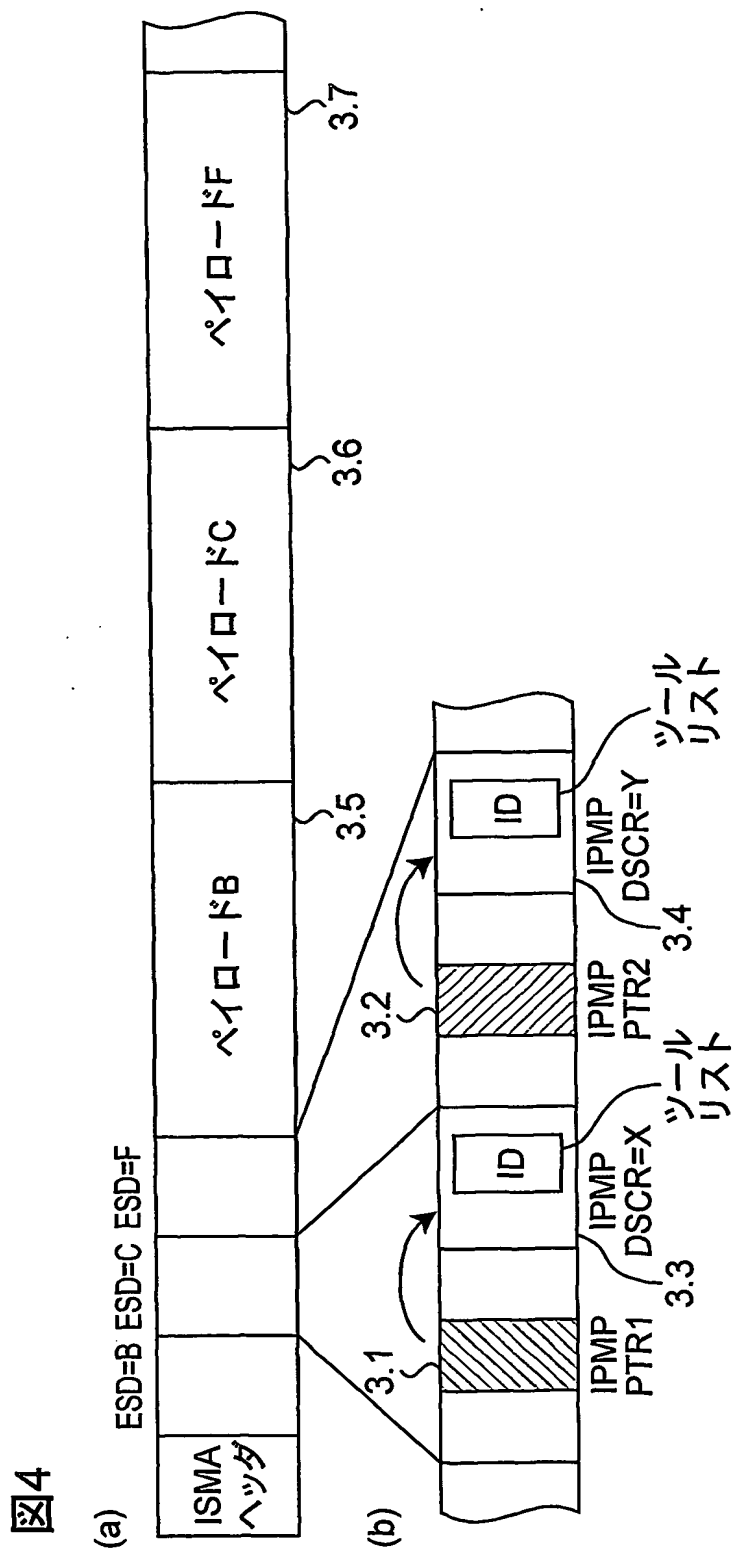
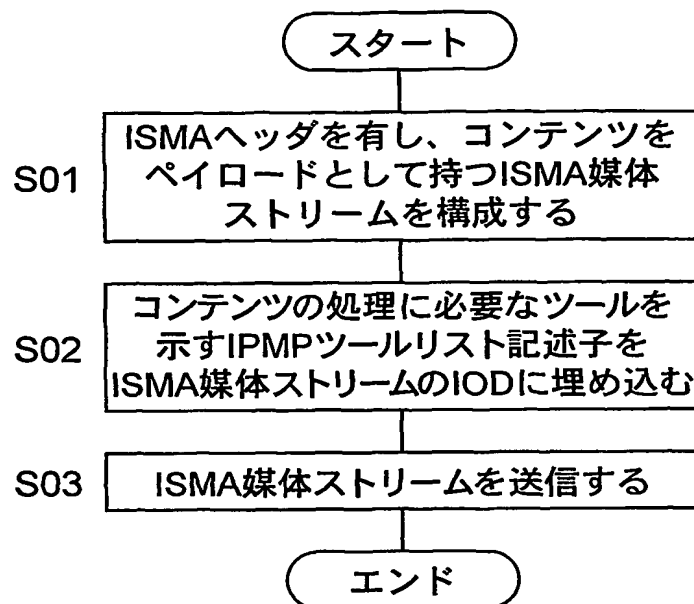


図6



6/8

図7

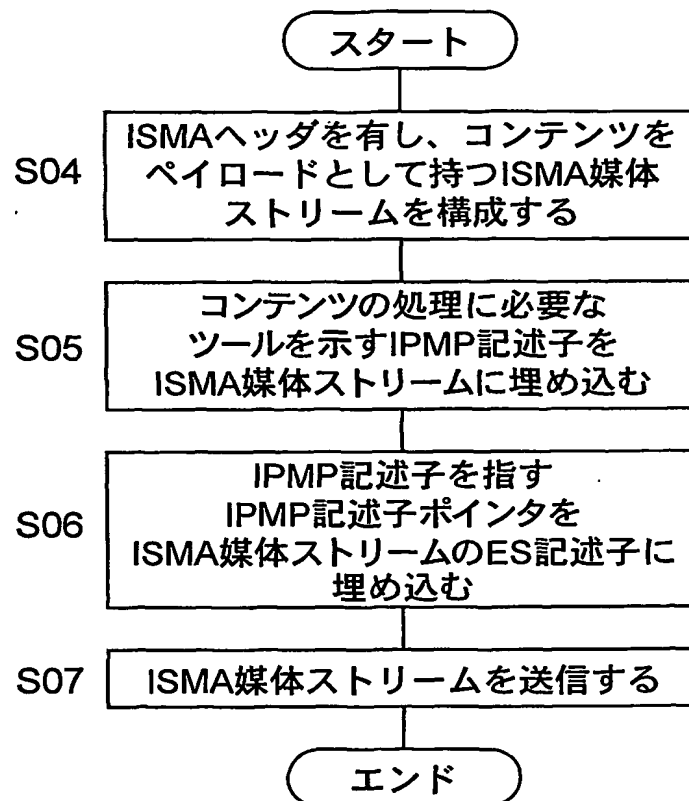


図8

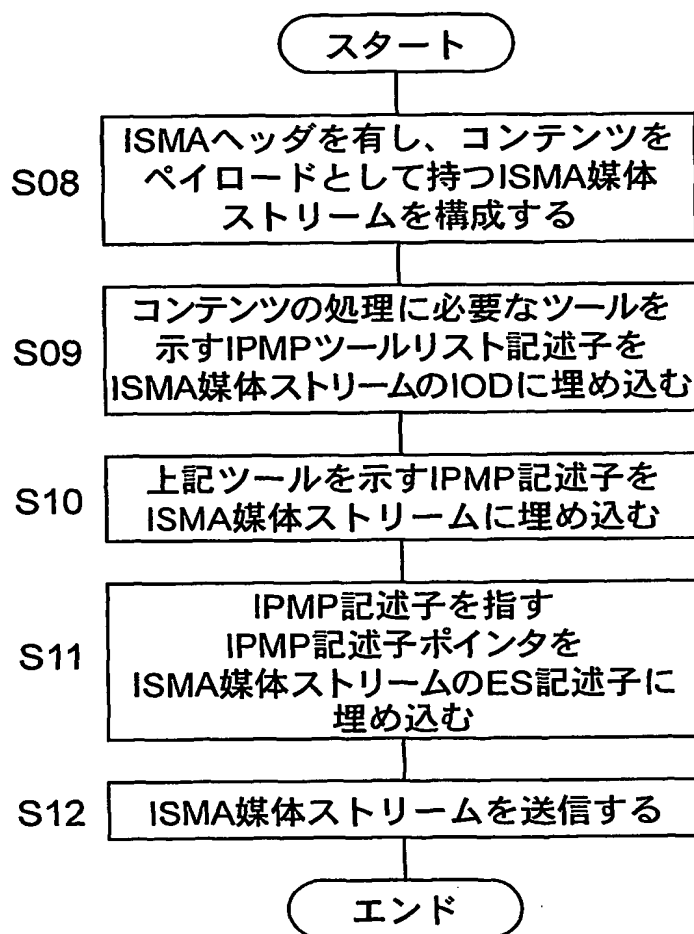
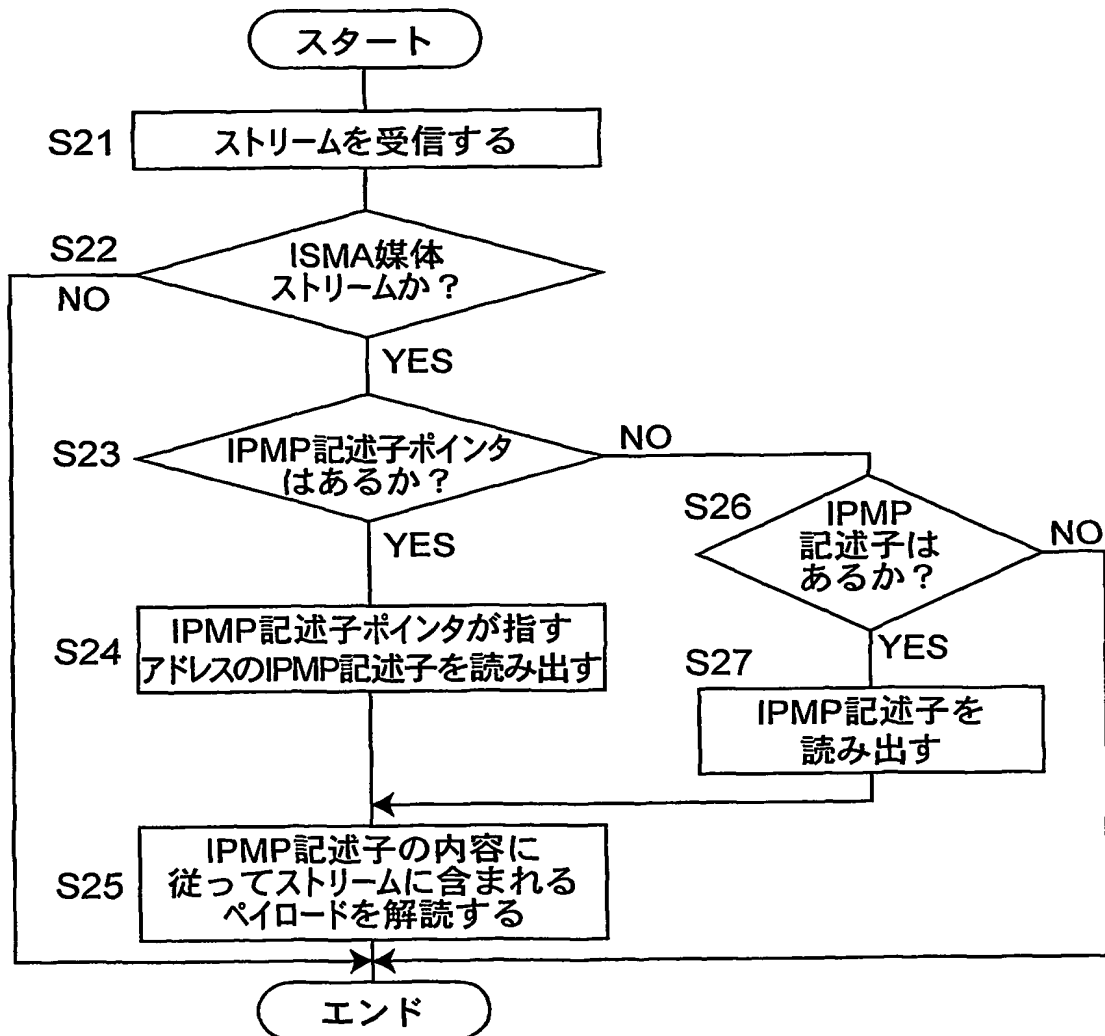


図9



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/006288

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L9/14, H04N7/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L9/14, H04N7/24

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST FILE (JOIS), WPI, MPEG-4, IPMP, ISMA

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, Y	Internet Streaming Media Alliance Encryption and Authentication Specification version 1.0 [online]., Internet Streaming Media Alliance, 03 March, 2004 (03.03.04), [retrieved on 06 September, 2004 (06.09.04)]., Retrieved from the Internet: <URL: http://www.isma.tv/resources/techspecs/ , http://www.isma.tv/resources/press/03September, 2003 (03.09.03)especially 7.3 Transport Pcket Structure, 8.4 IPMP Signaling .	1-9
Y	WO 99/48296 A1 (INTERTRUST TECHNOLOGIES CORP.), 23 September, 1999 (23.09.99), Page 21, line 15 to page 29, line 11 & CA 2425741 A1 & CN 1301459 A & EP 1062812 A1 & JP 2002-507868 A	1-9

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "&" document member of the same patent family

Date of the actual completion of the international search
08 September, 2004 (08.09.04)Date of mailing of the international search report
28 September, 2004 (28.09.04)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/006288

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MPEG-4 IPMP Extensions, Lecture Notes in Computer Science, Vol.2320, pages 126 to 140, 22 May, 2002 (22.05.02), especially 4.3 IPMP Tools Retrieval	1-9

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int.Cl⁷ H04L9/14, H04N7/24

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int.Cl⁷ H04L9/14, H04N7/24

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2004年
日本国登録実用新案公報	1994-2004年
日本国実用新案登録公報	1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICSTファイル (JOIS), WPI
MPEG-4, IPMP, ISMA

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
PY	Internet Streaming Media Alliance Encryption and Authentication Specification version 1.0 [online]. Internet Streaming Media Alliance, 2004.03.03, [retrieved on 2004-09-06]. Retrieved from the Internet: <URL:http://www.isma.tv/resources/techspecs/ http://www.isma.tv/resources/press/2003_09_03/> especially 7.3 Transport Pcket Structure, 8.4 IPMP Signaling.	1-9

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」 同一パテントファミリー文献

国際調査を完了した日

08.09.2004

国際調査報告の発送日 28.9.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

中里 裕正

5M

9364

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	WO 99/48296 A1 (INTERTRUST TECHNOLOGIES CORPORATION) 1999.09.23, 第21頁第15行-第29頁第11行 & CA 2425741 A1 & CN 1301459 A & EP 1062812 A1 & JP 2002-507868 A	1-9
A	MPEG-4 IPMP Extensions, Lecture Notes in Computer Science, Vol.2320, p.126-140, 2002.05.22, especially 4.3 IPMP Tools Retrieval	1-9